REMARKS

This responds to the Office Action mailed on March 16, 2005, and the references cited therewith.

Claims 12 and 13 are amended, no claims are canceled, and no claims are added; claims 1-35 remain pending in this application.

§101 Rejection of the Claims

Claims 1 and 3-31 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Claim 1 has been amended to make it clear that translation of the security policy is done by a computer. The resulting translated security policy is a tangible result which can be used by the security mechanisms to which it is exported.

Similarly, claims 14, 22 and 31 have been amended to make it clear that the method is a computer-implemented method.

No changes have been made to the system claims of claims 6-11. As noted in the MPEP at 2106.II.A, "[T]ransformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application of a mathematical algorithm, formula, or calculation, because it produces 'a useful, concrete and tangible result' -- a final share price momentarily fixed for recording and reporting purposes and even accepted and relied upon by regulatory authorities and in subsequent trades." *State Street*, 149 F.3d at 1373, 47 USPQ2d at 1601. Applicant describes, and claims in claims 6-13, a machine which translates a security policy into data which can be understood by the security mechanisms present in the system. Applicant respectfully submits that such a machine produces 'a useful, concrete and tangible result' as defined by *State Street*.

Applicant notes that the same section of the MPEP requires that when such a rejection is made, Office personnel must expressly state how the language of the claims has been interpreted to support the rejection. Applicant respectfully requests withdrawal of the rejection, or a more thorough discussion of why the Examiner feels the rejection should not be withdrawn.

§112 Rejection of the Claims

Claims 12-13 were rejected under 35 U.S.C. § 112, second paragraph, for indefiniteness. Claims 12 and 13 have been amended to correct the error in the claim language.

§102 Rejection of the Claims

Claims 1-3, 5-8, 11-19, 21-28, 30 and 32-34 were rejected under 35 U.S.C. § 102(a) as anticipated by Thomsen, O'Brien and Bogle ("Role Based Access Control Framework for Network Enterprises"), hereafter "Thomsen".

Thomsen describes a Role Based Access Control (RBAC) mechanism for managing access to a variety of network resources. As the Examiner notes, Thomsen describes a system in which application-specific security mechanisms are encapsulated into keys (Section 4.2) and the keys are linked to form key chains (Section 2.6). Thomsen states that key chains may contain other key chains.

As can be seen in Fig. 4 of the drawings, Applicant teaches that an RBAC model can be constructed that includes an application developer layer (30), one or more semantic layers (36) and a local system administrator layer 32. The goal of the application developer layer is to encapsulate application specific information so that it can be incorporated into the higher layers in a uniform manner. Once the application specific information has been encapsulated into an application key, it can be combined with other keys to form semantic layers 36 such as are shown in Fig. 7. Each layer 36 starts with a set of keys 40 and uses them to build up key chains 42 representing the policy at that level. Once key chains have been built, constraints 44 may be associated with them. The key chains for one layer become keys 40 of other layers 36. Within a layer 36 keys 40 are atomic units of policy. By drilling down to another layer 36 the user can determine how the key was composed.

The final layer of RBAC model described by Applicant is identical to the other layers except that at this level users can be associated with key chains. The top layer is the only layer where such user role binding takes place. The top layer is also assumed to be under the control of the local sysadmin. As noted above, the top layer is more dynamic than the lower layers as it must respond to the day-to-day operations of the network.

Applicant noted in the previous response that Thomsen does not consider, or even mention, the use of semantic layers to combine keys into key chains, as described by Applicant and claimed in claims 1-35. The Examiner disagrees, stating that "Thomsen discloses semantic layers (at 1, 1st para. & Fig. 1) ... to combine keys into key chains (Fig. 1 & Fig. 2)." The layers of Thomsen, however, are not used to combine keys into key chains and then to encapsulate key

chains as keys before passing the new keys to a different semantic layer as required by claims 1-5 and 14-35. Furthermore, Thomsen does not describe why or how one would encapsulate key chains as keys within a semantic layer or why or how one would pass the encapsulated chains to the next semantic layer. These features of an RBAC system are described by Applicant and claimed in claims 1-5, 14-35.

The Examiner stated that Thomsen discloses "encapsulating key chains (for example "Doctor" and "Nurse", Fig. 2) as keys ("Health Care Provider", Fig. 2) within a semantic layer (application)". Applicant respectfully disagrees. As noted in section 2.4, the "Health Care Provider" key actually has fewer permissions than either of the two keys that are purportedly the result of the encapsulation. That is contrary to the meaning and use of the claimed invention.

Furthermore, Thomsen does not describe the use of a plurality of semantic layers, wherein two or more of the semantic layers are used to encapsulate key chains as keys. In addition, Thomsen does not describe a user interface for defining a security policy as a function of keys received from a plurality of lower semantic layers as described by Applicant and claimed in claims 6-10.

Furthermore, Thomsen does not describe a tool for manipulating the RBAC model as described by Applicant and claimed in claims 11-13.

Reconsideration of all claims is respectfully requested.

Claims 1-35 were rejected under 35 U.S.C. § 102(a) for anticipation by Thomsen, O'Brien and Bogle ("Napoleon Network Application Policy Environment"), hereafter "Thomsen Napoleon". The authors of "Thomsen Napoleon" are the inventors in the present application. The article was not, therefore, "described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent," as required by 35 U.S.C. § 102(a).

Claims 1-4 and 32 were rejected under 35 U.S.C. § 102(e) for anticipation by Sandhu et al. ("The ARBAC97 Model for Role-Based Administration of Roles"). Applicant respectfully submits that 35 U.S.C. § 102(e) is limited to the use of patents issuing from patent applications filed before the filing date of another's patent application. Reconsideration and allowance of claims 1-4 and 32 is respectfully requested.

Even if Sandhu is considered a valid reference, it does not teach each of the limitations of claims 1-4 and 32. For instance, Applicant teaches at p. 9, that each security mechanism (e.g., a

firewall Access Control List or the mechanism to protect an FTP server on a Unix host) must be described as an abstract representation of rights associated with the security mechanism (the key). Claims 1-4 and 32 state that Applicant's method of defining and enforcing a security policy requires that one encapsulate "security mechanism application specific information for each security mechanism". Applicant is unable to find a teaching or suggestion in Sandhu that would lead one to encapsulate "security mechanism application specific information for each security mechanism" as defined by Applicant and claimed in claims 1-4 and 32. Reconsideration is respectfully requested.

§103 Rejection of the Claims

Claims 5-17, 21-26, 30 and 33-34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sandhu et al., as applied to claim 1 above, and in view of Varadharajan, Pato and Crall ("Issues in the Design of Secure Authorization Service for Distributed Applications"), hereafter "Crall".

Sandhu is described above.

Crall describes a RBAC system. Crall describes a system in which entitlements define access rights for principals. Profiles are used to provide the same privileges to groups or classes of principals. In the example given at page 879, an administrator creates a profile called Teller that defines all the privileges granted to bank tellers. A principal that becomes a member of the Teller profile automatically has all the privileges assigned in it. The Examiner stated that privileges "represent authorization to access application-specific resources" and that "entitlements" are "encapsulated privileges" that "represent authority to perform tasks".

As noted above, key limitations of claim 1 are missing from Sandhu and are not shown in Crall. Applicant respectfully suggests that claim 5 is patentable as dependent on claim 1 as described above.

With regard to claims 6-10, as noted in the discussion of claim 1 above, neither Sandhu nor Crall teach or suggest a security system having "a plurality of semantic layers, including a first semantic layer, wherein the two or more of the semantic layers combine keys into key chains, encapsulate the key chains as keys and export the keys to another semantic layer, wherein

each key encapsulates security mechanism application specific information for a security mechanism" as described by Applicant and claimed in claims 6-10.

With regard to claims 11-13, as noted in the discussion of claim 1 above, neither Sandhu nor Crall teach or suggest a security system having "a tool for manipulating the model, wherein the tool allows an administrator to: encapsulate security mechanism application specific information for each security mechanism, wherein encapsulating includes forming a key for each security mechanism; combine keys to form key chains; encapsulate key chains as keys within two or more semantic layers; pass the key chain keys to other semantic layers; form user key chains from the key chain keys; and associate users with the user key chains" as described by Applicant and claimed in claims 11-13.

Similarly, neither Sandhu nor Crall teach or suggest encapsulating key chains as keys within two or more semantic layers as described by Applicant and claimed in claims 14-31 and 33-35.

Claims 31 and 35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sandhu et al., in view of Crall, and further in view of Nyanchama et al. ("The Role Graph Model and Conflict of Interest").

As noted above, neither Sandhu nor Crall teach or suggest encapsulating key chains as keys within two or more semantic layers as described by Applicant and claimed in claims 14-31 and 33-35. Nyanchama does not teach or suggest encapsulating key chains as keys within two or more semantic layers as described by Applicant and claimed in claims 14-31 and 33-35.

CONCLUSION

For the reasons stated above, Applicant respectfully requests reconsideration of claims 1-35 and issuance of a Notice of Allowance. Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (612) 373-6909 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

DANIEL J. THOMSEN ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6909

Date September 16, 2005 By Thomas J. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 16th day of September, 2005.

THOMAS F. BRENNAN Thomas J. Brennan

Name Signature